2001

WebTrust Program: Security Principle and Criteria, January 1, 2001, Version 3.0

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

Chartered Accountants of Canada

Comptables agréés du Canada

AICPA/CICA

WebTrust SM/TM Program

Security Principle and Criteria

January 1, 2001

Version 3.0

The Principles and Criteria contained in this program supersede Version 2.0 of the WebTrust Principles and Criteria insofar as they relate to security and are effective for examination periods beginning after February 28, 2001. Earlier adoption is encouraged.

COMMITTEE AND TASK FORCE MEMBERS

AICPA
Assurance Services Executive Committee

Susan C. Rucker, *Chair*

Gari Fails

Ted Horne

Everett C. Johnson, Jr.

John Lainhart

J. W. Mike Starr

Wendy E. Visconty

Thomas E. Wallace

Neal West

Staff Contacts:

Alan Anderson,
Senior Vice President, Technical Services

Anthony J. Pugliese,
Director of Assurance Services

AICPA / CICA Electronic Commerce
Assurance Services Task Force

Everett C. Johnson, Jr., *Chair*

Bruce R. Barrick

Jerry R. DeVault

Joseph G. Griffin

Christopher J. Leach, *Vice Chair*

Patrick J. Moriarty

William Powers

CICA
Assurance Services Development Board

Doug McPhie, *Chair*

Diana Chant

Douglas C. Isaac

Marilyn Kuntz

Jeff Orchard

Frederick J. Phillips

David W. Stephen

Doug Timmins

Keith S. Vance

Staff Contacts:

Cairine M. Wilson,
Vice President, Innovation

Gregory P. Shields,
Director
Assurance Services Development

Kerry L. Shackelford

Donald E. Sheehy

Christian R. Stormer

Alfred F. Van Ranst

Staff Contacts:
Bryan Walker, CICA
Principal, Assurance Services Development

Sheryl Martin, AICPA
WebTrust Team Leader

CONTENTS

WEBTRUST SECURITY PRINCIPLE AND CRITERIA

Introduction

In the course of communicating and transacting business over the Internet, consumers and business must send and receive information about the other party. In most instances, parties who are interested in engaging in electronic commerce (e-commerce) will be anxious to ensure that the information they provide is available only to those individuals who need access to complete the transaction or follow-up on any questions that arise.

Information that is provided to another party is susceptible to unauthorized access during transmission over the Internet and while it is stored on the other party's computer systems. For example, personal information and credit card numbers may be intercepted by an unauthorized party while they are being transmitted over the Internet. However, if the information is encrypted, it is difficult for the unauthorized party to decipher it. Also, if the computer system where the data is stored is not protected by a firewall and a rigorous system of passwords, the information may be accessed by unauthorized personnel.

The WebTrust Security Principle sets out an overall objective for the security of data transmitted over the Internet and stored on an e-commerce system. In the course of a WebTrust audit, the practitioner uses the WebTrust Criteria as the basis for assessing whether the Principle has been achieved.

The WebTrust Security Principle

	The entity discloses its key security practices, complies with such security practices, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security practices.

The WebTrust Criteria[1]

The WebTrust Criteria are organized into four broad areas – disclosures, policies, procedures, and monitoring.

A four-column format has been used to present and discuss the criteria. The first column presents the criteria—the attributes that the entity must meet to be able to demonstrate that it has achieved the principle. The second, third and fourth columns provide illustrative disclosures and controls for business-to-consumer transactions, business-to-business transactions, and for transactions applicable to service providers. These are examples of disclosures the entity might make and controls that the entity might have in place to conform to the criteria. Alternative and additional disclosures and controls also can be used.

For the purpose of these criteria, the term "customer" includes (1) individual consumers who have provided information and consummated transactions and (2) business partners.

[1] These criteria meet the definition of "criteria established by a recognized body" described in the third General Standard for attestation engagements in the United States (AICPA, *Professional Standards*, vol. 1, AT sec. 100.14) and in the standards for assurance engagements in Canada (CICA *Handbook*, paragraph 5025.41).

WebTrust Principle and Criteria
Security

Principle

The entity discloses its key security practices, complies with such security practices, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security practices.

Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A Disclosures			
A.1 The entity discloses its security practices for providing access to its e-commerce system and data. Such disclosures should include practices for — • Registration and authorization of new users • Identification and authentication of authorized users • Maintaining and terminating authorized user access	You can register on line clicking on "Open a new account" and by providing your name, mailing address, telephone number and e-mail address. This information is encrypted using Secure Socket Layer (SSL) before being transmitted to us. We will e-mail you a user identification (ID) and password within twenty-four hours, which you can use to log in. You will be asked to change your password the first time you log in and every three months thereafter. You should choose a strong password that is difficult for others to guess and keep your password confidential. Your user ID and password will be deactivated if it is not used for six months.	This site requires the use of a digital certificate from the user to provide authentication, identification and encryption. Your digital certificate can be obtained from management by applying at www.mycertificate.com/ or you may email us at info@mycertificate.com. Your digital certificate will be valid for one year unless revoked sooner. We also require cookies to be set at the site to ease the use of this site and customize the Internet session. We place the following information in the cookie: identification number, product line and date. For more information go to www.mycertificate.com/cookie.html.	To obtain access to this system, a customer needs to complete an application and mail, e-mail or fax it to us. Upon approval of your credit, you will be provided with a user ID and a Secure ID token to allow access to the system. You can update the information on your application at any time, either by mail or on-line For additional information contact us at info@mysite.com.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.2	The entity discloses its procedure for individuals, companies or other users to inform the entity about breaches or possible breaches to the security of its e-commerce system(s).	Should you feel that there has been a breach to the security of this site please contact us *immediately* at (800) 123-1234.		
A.3	The entity discloses its procedures for customer recourse for issues that are not resolved by the entity regarding security. This resolution process should have the following attributes — • Management's commitment to use a specified third-party dispute resolution service or other process mandated by regulatory bodies, in the event the customer is not satisfied with the entity's proposed resolution of such a complaint together with a commitment from such third party to handle such unresolved complaints. • Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party.	Transactions at this site are covered by arbitration and arbitrated by the National Arbitration Forum. They can be reached at www.arb-forum.org or by calling toll free (800) 474-2371. For the details of the terms and conditions of arbitration, click here. Transactions at this site are covered by arbitration conducted through our designated arbitrator (name of arbitrator). They can be reached at www.name.org or by calling toll free (800) 111-2222. For the details of the terms and conditions of arbitration, click here. Transactions at this site are covered by the Banking (Canadian Banking) Industry Ombudsman of the Bankers Association who can be reached at www.bankom.org.xy or by calling toll free (800) xxx-xxxx. For transactions at this site, should you, our customer, require follow up or response to your questions or complaints, you may contact us at www.xxx.org. If your follow up or your complaint is not handled to your satisfaction, then you should contact the electronic commerce ombudsman who handles consumer complaints for e-commerce in this country. He can be reached at www.ecommercombud.org or by calling toll-free at (800) xxx-xxxx.		

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.4	The entity discloses any common applications, hardware, software, and other functionality that it offers for use by other individuals, users or groups, and the extent to which its security disclosures and controls address such functionality.	N/A	N/A	We provide on our Web site facilities for Web hosting and the use, by business customers, of the XYZ ERP software. The ERP software has a common configuration for application functionality and customized security configurations to meet the needs of each business customer. Our disclosures on this Web site and the related security controls include the common application functionality of the XYZ ERP software, but exclude the security features and controls that are customized for each business customer.

Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
B	**Policies**		
B.1	The entity's policies related to security cover the electric commerce system and include, but are not limited to, the following items: • Who is allowed access, what is the nature of that access, and who authorizes such access • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access • Who is accountable for security, system upgrades, backups, and maintenance • The type of scripts or programming that is permitted on served pages • Procedure to test and evaluate software, pages and scripts before they are installed • Controls over physical access to the system(s) • How complaints and requests about server and page content can be addressed • Procedures to handle security incidents • The entity's commitment to use third-party dispute resolution that conforms to the Principles of Arbitration for WebTrust	The Computer Security Policy (CSP) is fundamental to the existence and integrity of computer security of any organization. This document encompasses all aspects of security including such areas as — • Identifying threats and assets • Acceptable usage guidelines for users • Risk analysis • Identifying of authority figures • Procedures for day-to-day and other incidental security operations Qualified users can obtain the complete document for review.	Our company's defined security policy details access privileges, information collection needs, accountability, and other such matters. It is reviewed and updated at quarterly management meetings and undergoes an intense review on an annual basis by the Information Technology (IT) department. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service level agreements. For example, current policy prohibits shared IDs; each support person has his or her own unique ID to log on and maintain network equipment. A complete policy with details regarding access, scripting, updates, and remote access are available for review by qualified personnel. This document will not be released to the general public for study.	The company's security policy details access privileges, hardware and software modification procedures (including updates), Web access and Web posting. In addition, strict procedures are in place to control logical as well as physical access to the system. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service level agreements. Current policies prohibit shared IDs. Each support person has his or her own unique ID to log on and maintain network equipment. A complete policy with details regarding access, scripting, updates, and remote access are available for review by qualified personnel. This document will not be released to the general public for study.
B.2	The employees responsible for security are aware of and follow the entity's policies related to security.	The company's policies relating to security are reviewed with new employees as part of their orientation and the key elements of the policies and their impact on the employee are discussed. New employees must then sign a statement signifying that they have read, understand and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with these policies.		

Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
B.3 Accountability for the entity's policies related to security has been assigned.	Management has assigned responsibilities for the enforcement of the company security policy to the chief information officer (CIO). Others on the executive committee assist in the review and update of the policy as outlined in the executive committee handbook.		
B.4 The entity has allocated training and other resources to support its policies related to security.	The company has budgeted for security training for the IT department. This amount is reviewed quarterly to ascertain whether additional training is needed based on employee feedback as well as changes in security.	The company has a quarterly scheduled training for all key IT employees. The IT department is also charged with holding quarterly security updates for all company employees as it relates to the employee's job function. The CIO oversees this responsibility and reports to the executive committee on a regular basis.	Management has an on-going security training program for all employees. IT staff is required to submit an annual training request based on job description. All employees are given periodic security training courses put on by the IT department. The CIO evaluates these programs and makes a quarterly report to the executive committee.
B.5 The entity's policies related to security are consistent with disclosed security practices and applicable laws and regulations.	Management reviews its disclosed security policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. Management makes any changes or needed modifications to the policy or disclosure within five business days of its evaluation. Laws and regulations that affect the disclosed site security policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update.		

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C	**Procedures**			
C.1	The entity has security procedures to establish new users.	New users are given a secure session in which to provide new user information and select an appropriate user ID and password.	New users are given a secure session in which to provide new user information and select an appropriate user ID and password. Passwords must contain at least six characters, one of which is non-alphanumeric.	New users provide information in a Secure Socket Layer (SSL) session. User IDs and passwords are provided to the user and contain non-alphanumeric characters.
C.2	The entity has security procedures to identify and authenticate authorized users.	All users are required to provide a unique user ID and password to place an order or access their specific customer information.	To enter the site all customers are required to provide a unique user ID and password. These passwords are case sensitive and need to be updated every ninety days. Users are required to use the digital ID provided by the company to access, place or update orders. File and directory level user and group permissions are used to further restrict access based on information contained within the digital certificate.	System level access to all production systems (UNIX and Windows NT) is provided via a strong identification and authentication mechanism (digital ID, one-time password, SecureID or other system). Strong, static passwords are used for systems that do not require a strong identification and authentication mechanism. Controlled access by a software authentication product with a strong identification and authentication mechanism is required for access to any routers.
C.3	The entity has procedures to allow users to change, update, or delete their own user profile.	To update, change or delete user information, the user's current ID and password are required. After providing this information in a secure session, the user can proceed to the user profile section for any changes.	The user can process changes to a user profile only after a processing code is obtained from the entity. This code is obtained after verification with the user's company about the need for the update or change.	All changes to user profiles are done after providing user ID and password. The only changes allowed are updates to the user ID and password. Changes to personal information or deletions must be processed in writing.

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C.4	The entity has procedures to limit remote access to the internal network to only authorized personnel.	Logical access restrictions (for example, firewalls, routers and password controls) are maintained by the IT department. These controls are tested on a periodic basis by performing penetration testing from both within the internal network and from the Internet. Remote access is provided to key employees; the system accepts remote calls, verifies the user, and then hangs up and calls the user back at the authorized number. Identification and authentication is accomplished through the combination of a user ID and one-time password.		The remote access to and use of the computing resources are restricted by the implementation of an authentication mechanism for identified users and resources associated with access rules. User IDs and passwords are stored in an encrypted database with the associated encryption key stored off-line.
C.4.1	The entity has procedures to protect internal systems from viruses and malicious code.	The company maintains anti-virus software on its systems, updates its virus signatures at least monthly, and takes reasonable precautions to protect both its systems and the customer's computer from viruses during the e-commerce session.	In connection with other security monitoring, management participates in user groups and subscribes to services relating to computer viruses. Daily the server downloads the most current virus definitions and any updates are then automatically "pushed" to users as they log on. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.	Management subscribes to several services relating to viruses and other malicious codes. The service provider's systems run two separate virus scanning programs at all times that are updated daily. Internal users are required to run a full scan on their local machines once a month.

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C.4.2	The entity has procedures to prevent unsecured dial-up access to the Internet during active local area network session(s).	If an employee of the entity attempts to use a dial-up connection to access the Internet (rather than use the network connection), the system drops the network connection until the dial-up session is terminated. The session address is transmitted to the security officer for follow-up.		
C.4.3	The entity has procedures to minimize or eliminate unneeded network services (port numbers).	The entity reviews on a monthly basis all services offered by the system (for example, file transfer protocol (ftp) and Telnet) and eliminates those not needed.	A listing of the needed server services (for example, telnet, ftp and hypertext transfer protocol (HTTP)) is maintained by the IT department. This list is reviewed by company management on a routine basis for its appropriateness for the current operating conditions. A port scan is done at least monthly and compared with the approved list. Any variations are reported to management within twenty-four hours for follow-up.	
C.4.4	The entity has procedures to update software to optimal versions and patches on a timely basis.	The entity has relationships with all key systems vendors and is notified via email when a new update is available.	The IT department maintains a complete listing of all software and the respective level and patch. Management meets (via email, telephone, or in person) with its technology vendors on a regular basis to ascertain current software release and patch levels and the associated security issues. Management then makes a determination with consultation from vendors as to the optimal software release and patch level.	On a monthly basis, the service provider obtains notification from the software vendors of the current release, version number, and patch level. With consultation and information from reputable outside security information sources (for example, Computer Security Resource Clearinghouse, Computer Incident Advisory Council), management makes a determination about optimal software and patch level based on the current operating environment.

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C.5	The entity has procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information.	Customers are required to enter a user ID and password to access personal information and orders. A challenge word or phrase (for example, favorite sport or music – not a word that is easily identifiable such as mother's maiden name) is stored on the system in the event a user forgets or misplaces a password.	All access to customer accounts is restricted to the customer through the use of a unique digital certificate associated with each customer. Customer sessions between the browser and e-commerce systems are protected to avoid other users from hijacking a customer's session (for example, use of unique digital certificates or cookies checking for random unique identifiers before the start of each session).	One-time passwords, smart cards, or both restrict all system access from outside the entity, other than for customary e-commerce transactions through the Web page. Customer Web sites hosted by the Internet service provider (ISP) are prevented from intercepting messages not addressed to them. Packet filters are implemented on the ISP Internet gateway routers using access control lists (ACLs) according to the ISP firewall policy. Anti-spoof filters are used on the routers to prevent spoofing of trusted sources. Additional ACLs are used to control customer access to only their network segments. The various local area networks (LAN) segments are firewalled from the rest of the networks.
		The authentication process allows the user to access only information relevant to that particular user. Other methods are in place to detect users attempting to guess another password or if a brute force attack is under way. If such an attack is detected, the system disconnects from the user and reports the security breach for follow-up.		
C.6	The entity has procedures to limit access to systems and data to only authorized employees based upon their assigned roles and responsibilities.	Employee access to customer data is limited to individuals based upon their assigned responsibilities. Idle workstations are "timed-out" after thirty minutes. Access to the corporate information technology facilities is limited to authorized employees by use of a card/key system supported by video surveillance monitoring.		

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C.6.1	The entity has procedures to safeguard master or "super user" passwords and restricts access to such passwords to a limited number of authorized personnel.	Master or super user passwords are known only by authorized systems administrators. For emergency situations, these and other key passwords are written down, placed in a marked envelope and stored in the company safe that is accessible only by the chief information officer (CIO), chief financial officer (CFO), and chief executive officer (CEO).		System passwords and other key passwords are encrypted and stored in the company safe under dual control. Strict policy requires that these passwords can be accessible by only at least two of the following: CIO, CFO and CEO.
C.6.2	The entity has procedures to minimize access to idle workstations by unauthorized personnel.	Customers visiting the site are automatically redirected to unsecured (non-SSL) pages after a specified period of inactivity. A logout utility runs continuously on the system. It scans the network for idle workstations and logs them off after 10 minutes of inactivity. Company employee workstations automatically log off the network after a specified period of inactivity.		
C.6.3	The entity limits physical access to firewalls, servers and other critical system(s) to authorized personnel.	Physical access to the servers and related hardware (for example, firewalls and routers) is controlled and monitored by video surveillance.		
C.6.4	The entity secures its programs and data during the backup, off-site storage, and restoration processes.	During the daily backup routine, the data is secured from both physical and logical access by unauthorized personnel. During any restoration process, no access is allowed by unauthorized personnel.		
C.7	The entity uses encryption or other equivalent security procedures to protect transmissions of user authentication and verification information passed over the Internet.	The company uses 128-bit SSL encryption for all transmission of private or confidential information, including user ID and password. Users are also encouraged to upgrade their browser to the most current version to avoid any possible security problems. The company does not use encryption for authentication purposes, but uses one-time passwords or tokens to authenticate users.		

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C.8	The entity has procedures to maintain system configurations that minimize security exposures.	Company management routinely evaluates the level of performance it receives from the ISP that hosts the company Web site. This evaluation is done by evaluating the security controls the ISP has in place by an independent third party as well as by following up with the ISP management on any open items or causes for concern.		The service provider meets with its technology vendors on a regular basis (for example, SUN, Cisco and Microsoft). Identified vendor security issues are documented and conveyed to the vendor to the appropriate level of management, depending on the severity of the exposure and risks associated with its planned or current deployment in the network. All vendor security issues are associated with agreed upon time frames and followed up on by an ISP representative.
C.9	The entity has procedures to monitor and act upon security breaches.	System logs are monitored and evaluated on a daily basis. Monitoring software is in place that notifies the IT manager via e-mail and pager should any incident be in progress. If an incident occurs a report is filed within twenty-four hours for follow-up and analysis. Customers are directed to an area of the Web site to post a message about security breaches or possible breaches as soon as they become concerned. These customer comments are followed up within twenty-four hours for evaluation, a report is issued to the customer, and CIO or the customer may contact the incident response hot-line by telephoning (888) 911-0911 24X7.		
C.10	The entity has established and adheres to programming standards and conducts software testing in a controlled environment to ensure Web pages using active content technologies (for example, Java applets, ActiveX and JavaScripts) are not susceptible to security weaknesses.	The company's systems development methodology describes the software development and maintenance processes, and the standards and controls that are embedded in the processes. These include programming and testing standards.	Current policy prohibits the copying of applets, scripts, or other active content from other sites. All pages and other programs are placed on a staging server for testing before being placed on the main server. Management subscribes to current security publications that evaluate these technologies.	

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
D	**Monitoring**			
D.1	The entity has procedures to monitor the security of its e-commerce systems and to identify any need for changes to its security procedures.	The information security group uses the following monitoring tools: • COPS – This software provides a snap shot of the system which is analyzed on a monthly basis. • Tripwire – This is a real time monitor which is used to detect intruders. • SATAN – This software is run monthly and provides a security analysis of the system. In addition the group maintains and analyzes the server logs.	Commercial and other monitoring software (for example, COPS, SATAN and ISS) is run on a routine basis. The report outputs from these programs are analyzed for potential weaknesses and threats to the systems. Changes are made due to the information contained in these reports and with the consultation and approval of management.	
D.2	The entity has procedures to monitor its security incident procedures and update these as needed due to technology changes, changes in the structure of the e-commerce system(s), or other information.	Weekly IT staff meetings are held to address current security concerns and their findings are discussed at quarterly management meetings.	Senior management reviews the security policy on a biannual basis and considers developments in technology and the impact of any laws or regulations.	
D.3	The entity has procedures to monitor environmental and technology changes and related risks and their impact on its security practices.	A risk assessment has been prepared and is reviewed on a regular basis or when a significant change occurs in either the internal or external environment. Changes in system components are assessed for their impact on documented system security objectives, policies and standards.		

Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
D.4 The entity has procedures to provide that reports of noncompliance with security disclosures and controls are promptly addressed and that corrective measures are taken on a regular and timely basis.	Security issues are recorded and accumulated in a problem report. Corrective action is noted and monitored by management.		

APPENDIX A

WEBTRUST SM/TM SELF-ASSESSMENT QUESTIONNAIRE

FOR SECURITY

This questionnaire is for use by electronic commerce (e-commerce) service providers to document their security disclosures, policies, procedures and monitoring for e-commerce as a basis for their assertion or representation that "on its Web site at www.___.____ during the period _____, 200_ through _____, 200_ the entity —

- Disclosed its key security practices for electronic commerce,
- Complied with such security practices, and
- Maintained effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security practices

based on the AICPA/CICA WebTrust SM/TM Criteria."

General Information

E-commerce Activities to Be Covered

1. Describe as applicable:

   a) The goods and services being sold or provided?

   b) The typical customer?

   c) The typical form of payment?

2. What is the Web site URL?

3. Identify the individual who has primary responsibility for controlling the online disclosure of the entity's policies and its adherence to these policies and what is this individual's reporting relationship to the entity's management?

4. How long has the entity been selling such goods and services through this form of e-commerce?

5. Has the entity made substantive changes to its disclosed policies and practices or the related disclosures in the last ninety days? If so, describe the nature of such changes and when each change occurred.

Information Systems Used to Support E-commerce Activities

6. List the Web Site or other customer interface systems and provide the following information about each:

    a) Provide a description.

    b) Indicate who, in this entity, is responsible.

    c) Describe any portion of these systems that is outsourced to third parties.

    d) Describe the frequency and nature of changes to Web site and customer interface systems.

7. List the telecommunications and network systems, including the following information.

    a) Give a description.

    b) Indicate, who, in this entity, is responsible.

    c) Describe any portion of these systems that is outsourced to third parties.

    d) Describe the frequency and nature of changes to telecommunications and network systems.

8. List the other supporting systems and technology, including the following information.

    a) Provide a description.

    b) Indicate who, in this entity, is responsible.

    c) Describe any portion of these systems that is outsourced to third parties.

    d) Describe the frequency and nature of changes to such systems and technology.

Web Site Server Technology

9. Describe the e-commerce server platform(s) in use (description and version).

10. How many e-commerce servers are in use at the primary site? How many are at an alternate or backup site?

11. Is SSL used for some, or all, Internet transactions? If so, describe the kinds of transactions for which SSL is used and the kind of digital server certificate being used.

12. Identify the technical staff (and/or whether the site is hosted by an ISP and the technical staff of the ISP) who are capable of performing the following technical tasks:

a) Generate a Certificate Signing Request (CSR) using the Web server software?

b) Install a Digital Certificate (also known as a Digital ID) on the Web server software?

c) Configure certain pages on your web server to be secure using (SSL)?

d) Install a Java Applet on the appropriate Web page?

13. Identify:

a) The WebServer package used.

b) Identify the version of Netscape that your customer base is most likely to be using.

Control Environment

14. Describe the factors in the entity's organization that contribute to a control environment that is generally conducive to reliable disclosures on its Web site and effective controls over monitoring the entities compliance with its disclosed privacy policies. Such factors might include, but are not limited to the following:

a) Management's "tone at the top"

b) Hiring, development, and retention of competent personnel

c) Emphasizing the importance and responsibilities for sound practices and effective control

d) Supervising its e-commerce related activities and control procedures

e) Employing a suitable internal auditing function that periodically audits matters related to the entity's e-commerce policies

f) Other factors

Security Specific

A Disclosures

1. Does the entity disclose its security practices for providing access to its e-commerce system and data including:

a) Registration and authorization of new users

b) Identification and authentication of authorized users

c) Maintaining and terminating authorized user access.

2. Does the entity disclose the procedures for individuals, companies or other users to report breaches or possible breaches to the security of its e-commerce system(s)?

3. Does the entity disclose its procedures for customer recourse for issues that have not been resolved by the entity regarding security? This resolution process should have the following attributes:

   a) Management's commitment to use a specified third-party dispute resolution service or other process mandated by regulatory bodies, in the event the customer is not satisfied with the entity's proposed resolution of such a complaint together with a commitment from such third party to handle such unresolved complaints.

   b) Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party.

4. Does the entity disclose any common applications, hardware, software, and other functionality that it offers for use by other individuals, users or groups, and the extent to which its security disclosures and controls address such functionality?

B Policies

1. Does the entity's policies related to security cover the e-commerce system and include at least the following:

   a) Who is allowed access, what is the nature of that access, and who authorizes such access.

   b) Procedures to add new users, modify the access levels of existing users, and remove users who no longer need access.

   c) Identify the individual responsible for security, system upgrades, backups, and maintenance.

   d) The type of scripts or programming that is permitted on served pages.

   e) Procedure to test and evaluate software, pages and scripts before they are installed.

   f) The controls over physical access to the system(s).

   g) How complaints and requests about services and page content can be addressed.

   h) Procedures to handle security incidents.

   i) The entity's commitment to use third-party dispute resolution that conforms to the Principles of Arbitration for WebTrust?

2. How are the employees responsible for security made aware of and required to follow the entity's policies related to security?

3. Identify the individual responsible for the entity's security policy.

4. Has the entity allocated training and other resources sufficient to support the entity's policies related to security?

5. Are the entity's policies related to security consistent with disclosed security practices and applicable laws and regulations?

C Procedures

1. Does the entity have security procedures to establish new users?

2. Does the entity have security procedures to identify and authenticate authorized users?

3. Does the entity have procedures to allow users to change, update, or delete their own user profile?

4. Does the entity have procedures to limit remote access to the internal network to only authorized personnel?

    a) Does the entity have procedures to protect internal systems from viruses and malicious code?

    b) Does the entity have procedures to prevent unsecured dial-up access to the Internet during active local area network session(s)?

    c) Does the entity have procedures to minimize or eliminate unneeded network services (port numbers)?

    d) Does the entity have procedures to update software to optimal versions and patches on a timely basis?

5. Does the entity have procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information?

6. Does the entity have procedures to limit access to systems and data to only authorized employees based upon their assigned roles and responsibilities?

    a) Does the entity have procedures to safeguard master or "super user" passwords and restrict access to such passwords to a limited number of authorized personnel?

    b) Does the entity have procedures to minimize access to idle workstations by unauthorized personnel?

    c) Does the entity limit physical access to firewalls, servers and other critical system(s) to authorized personnel?

d) Does the entity secure its programs and data during the backup, off-site storage, and restoration processes?

7. Does the entity use encryption or other equivalent security procedures to protect transmissions of user authentication and verification information passed over the Internet?

8. Does the entity have procedures to maintain system configurations that minimize security exposures?

9. Does the entity have procedures to monitor and act upon security breaches?

10. Has the entity established and does it adhere to programming standards and does it conduct software testing in a controlled environment to ensure Web pages using active content technologies (for example, Java applets, ActiveX and JavaScripts) are not susceptible to security weaknesses?

D Monitoring

1. Does the entity have procedures to monitor the security of its e-commerce systems and to identify any need for changes to its security procedures?

2. Does the entity have procedures to monitor its security incident procedures and to update these as needed due to technology changes, changes in the structure of the e-commerce system(s), or other information?

3. Does the entity have procedures to monitor environmental and technology changes and related risks and their impact on its security practices?

4. Does the entity have procedures to provide that reports of noncompliance with security disclosures and controls are promptly addressed and that corrective measures are taken on a regular and timely basis?